



Analysis of Evidence

For DHS/ICE Operation "Tangled Web" – Target
Name(s): Jeffrey J. Reichert (FallsInc.com)

CONFIDENTIAL

Prepared by Jason Allen, Internet Anti-Piracy Specialist
Nintendo of America Inc.



Table of Contents

I. Overview	
A. Document Summary	Page 3
B. Terminology & Definitions	Page 3
II. Analysis of Evidence	Page 4
III. Explanation of <i>Wii</i> Video Game Console Technological Protection Measures	Page 5
IV. Conclusion	Page 8



Analysis of Evidence for DHS/ICE Operation "Tangled Web"

I. Overview

A. Document Summary

This document contains the results of the analysis of evidence, including both seized products and products purchased through undercover investigation, from the Department of Homeland Security/Immigration and Customs Enforcement Operation "Tangled Web."

At the request of the above named agency, the evidence was analyzed by two Nintendo of America Inc. representatives on Wednesday, August 17th, 2011 at the DHS/ICE office located at 8370 Dow Circle W., Strongsville, OH 44136. The conclusions found and stated in this document are based upon the technical expertise of Jason Allen (an internet anti-piracy specialist with over 10 years of experience in investigating internet piracy cases for multiple IP industries) and Dylan Rhoads (a senior engineer with over 10 years of experience in video game software/hardware design).

B. Terminology & Definitions

In this document there are a variety of terms used to describe various topics in internet anti-piracy enforcement, and more specifically, video game products. Definitions for each term are included below.

Video game console/handheld: A video game console is a hardware device that produces audiovisual signals when connected to a display device (usually a television or monitor). These signals are interpreted by the game controller devices supplied with the video game console to enable a user to interact and play the video game content. A video game handheld console is a hardware device that combines the game controller device and display device into the hardware in a small form factor designed for being held in a user's hands. For the purposes of this analysis, the video game consoles being discussed are the Nintendo GameCube and Nintendo Wii, and the video game handheld console being discussed is the Nintendo DS. The above named video game consoles use proprietary disc-based media for their video games, while the above named handheld uses proprietary cartridge media for its video games.

Mod Chip: A "modchip" (shorthand for modification chip) is a small electronic device (often a microchip) used to circumvent the security technologies built into video game hardware. These security technologies are added by the console manufacturer to protect the copyrighted content within the console and to ensure that only legitimately produced and distributed video games interoperate with the console. A modchip will either disable or bypass these technologies to allow the play of unauthorized and illegally created pirate or counterfeit copies of video games.



Analysis of Evidence for DHS/ICE Operation "Tangled Web"

Game Copiers: "Game Copiers" (also referred to as "Flash Cards") are small cartridges which are often produced in the exact same size and shape as a legitimate cartridge for a Nintendo DS handheld console. They have a slot for a Micro-SD flash memory card which can hold copied game data. Users will acquire pirate copies of legitimate DS games from internet piracy sources and then load them onto the Micro-SD card and insert it into the game copier. Game copiers are most often shipped by their manufacturers with software pre-loaded on the cartridge that will circumvent security technologies on the DS handheld console, thereby allowing playback of the pirated game data.

II. Analysis of Evidence

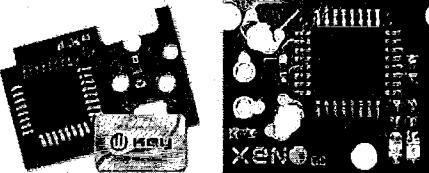
In order to verify the infringing nature of the seized evidence, the Nintendo employees examined the evidence using their expertise on Mod Chips and Game Copiers, and where applicable, tested the evidence to confirm that it worked—by loading pirated copies of games and thereby demonstrating successful circumvention of security technologies within the video game consoles/handheld consoles.

A complete list of all evidence analyzed by the Nintendo representatives is included below. Each set of evidence is classified in its own table with details regarding:

- **CASE # – This is the Incident or FPF Evidence # that appeared on the bag/box/container holding the evidence**
- **URL – This is the URL of the website from which the evidence was acquired (where applicable)**
- **Defendant Name – The name of the Defendant that appeared on the bag/box/container holding the evidence (where applicable)**
- **Infringing Products – The list of infringing products in evidence**
- **Evidence Review Comments – More information regarding the evidence examination**



Analysis of Evidence for DHS/ICE Operation "Tangled Web"

<u>CASE (Incident/FPF Evidence #)</u>	<u>Evidence Review Comments</u>
2007SZ007041601	
<u>URL</u>	
fallsinc.com	
<u>Defendant Name</u>	
Jeffrey J. Reichert	
<u>Infringing Product(s)</u>	
10 Wii Key Mod Chips, 1 Xeno (GameCube) Mod Chip	<p>The evidence bag for this case # contained: 11 small microchips. They were examined and determined to match the exact physical characteristics (color, shape, size, circuit layout) of the Wii Key and Xeno GC mod chips, respectively (pictured below).</p> 

<u>CASE (Incident/FPF Evidence #)</u>	<u>Evidence Review Comments</u>
2007SZ005938901	
<u>URL</u>	
fallsinc.com	
<u>Defendant Name</u>	
Jeffrey J. Reichert	
<u>Infringing Product(s)</u>	
1 Wii Console Hard-Modded with Wii Key Mod Chip	<p>This evidence box for this case # contained: 1 Nintendo Wii Console marked as modified with a Wii Key mod chip. The console was connected to a TV for testing to verify that the console was modified with a modchip. Upon placing a pirated copy of Super Paper Mario (the game was on a DVD-R format optical disc and provided as part of other evidence by law enforcement) in the Wii console, the game loaded correctly, confirming that the console had been modified with the Wii Key mod chip and was infringing.</p>

III. Explanation of *Wii* Video Game Console Technological Protection Measures

How the *Wii* Video Game System Works

The Nintendo *Wii* video game system was launched in December 2006. A basic *Wii* video game system is comprised of the *Wii* video game console, the *Wii* controller and *Wii* video game software issued in (optical) disc format for playing on the *Wii* video game console. This *Wii* video game software and much of the game software played on the *Wii* video game console is copyright protected. In order to play *Wii* video game software, the player first connects the *Wii* video game console to a television. Then the player can insert a *Wii* video game disc issued by Nintendo (or a developer licensee) into the *Wii* video game console. The console will recognize and play the *Wii* video game disc.



Analysis of Evidence for DHS/ICE Operation "Tangled Web"

As the game plays, the *Wii* video game console loads the appropriate part of the software program stored in the *Wii* video game disc onto the system memory of the *Wii* video game console, and this allows the game to be played by converting the software code in the system memory into moving images on the television screen. The player can control the movement of the images by use of a controller.

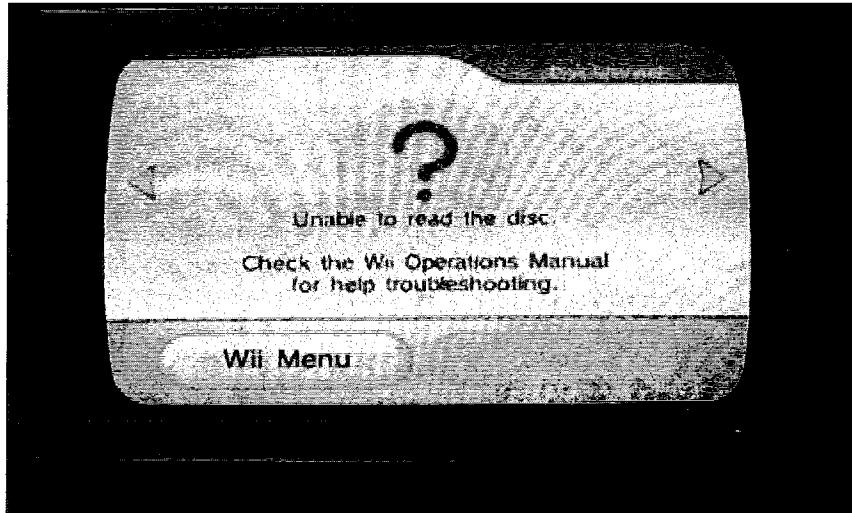
Nintendo and its developers have issued and continue to issue a large number of game software titles for use with the *Wii* video game console.

Technological Protection Measures in the *Wii* Video Game System

Nintendo incorporates into its *Wii* video game console several effective technological protection measures to control the access to and use of *Wii* video games. These measures are designed to prevent the *Wii* video game console from playing counterfeit copies of *Wii* video games. All Nintendo *Wii* video game discs contain the so called "*Wii* Copy Protection Code" which is stored in a copy protected area of the *Wii* video game discs and can therefore not be copied with a regular DVD writer. Even with respect to those games developed by licensee publishers for the *Wii* video game console, Nintendo issues copy protection codes for those games.

Each time a disc is put into a *Wii* video game console and played, the console will always look for the *Wii* copy protection code contained in authentic *Wii* video game discs first, before any *Wii* game data is loaded from the inserted disc into the system memory of the *Wii* video game console. If the *Wii* Copy Protection Code is not found, the disc cannot be played. The following warning notice will appear on the TV screen:

"Unable to read the disc. Check the *Wii* Operations Manual for help or troubleshooting."





Analysis of Evidence for DHS/ICE Operation "Tangled Web"

A disc which does not contain the *Wii* copy protection code therefore cannot be played by the *Wii* video game console.

How *Wii* Mod Chips Work

A "mod chip" or "modification chip" is a semiconductor chip which, when affixed to the printed circuit board of the *Wii* disc drive of the *Wii* video game console, enable the users to play unauthorized copies of *Wii* video game discs on the modified *Wii* video game consoles.

Mod Chips circumvent the above described technical protection measures (TPM) by the following means:

a. *Wii* Disc Drive TPM

Mod chips circumvent the *Wii* disc drive TPM by modifying the firmware of the *Wii* disc drive. Once the mod chip has modified the *Wii* disc drive's firmware, the drive can read common DVD-R discs.

b. *Wii* Copy Protection Code TPM

Some mod chips circumvent the *Wii* Copy Protection Code TPM by disabling the *Wii* Copy Protection Code check routine of the *Wii* video game console.

These mod chips are installed after disassembling the console and, sometimes, after removing part of its components; in many cases independent retailers may offer to install the mod chips themselves in the console to be modified, or even directly offer the already modified *Wii* video game console for sale.

When a game disc, regardless of whether it is a genuine or illegal copy, is inserted into a modified *Wii* console, the copyright protected computer program and other creative works (or substantial parts of them) are read from this game disc and copied into the console system memory. In effect, this produces an unauthorized copy of the copyright protected digital data from that game disc within the modified *Wii* video game console.

Pirated/counterfeit *Wii* video game discs can be played on a *Wii* video game console after installation of the modification chip.

*****This tutorial was updated by Nintendo of America Inc. on February 15th, 2012*



Analysis of Evidence for DHS/ICE Operation "Tangled Web"

IV. Conclusion

The evidence examined in this case, as detailed in Section II of this report, revealed that those products, technologies, services or devices circumvent the technological protection measures employed by Nintendo to effectively protect copyrighted works. These products, technologies, services or devices have only limited commercially significant purpose or use other than to circumvent Nintendo's technological protection measures.